U.S. ARMY EVALUATION CENTER

Cybersecurity vs. Cyber Survivability: A Paradigm Shift

March 30, 2017

BLUF

- The T&E community should stop using the term “cybersecurity” when what we mean is “cyber survivability”

blogtalkradio.com

Agenda

- What we really want to find out from T&E
- Definitions of key terms
- Limitations of the term “Cybersecurity”
- Cyber Survivability
- System Survivability KPP Cyber endorsement
- Proposed COIC
- Conclusion
- Questions

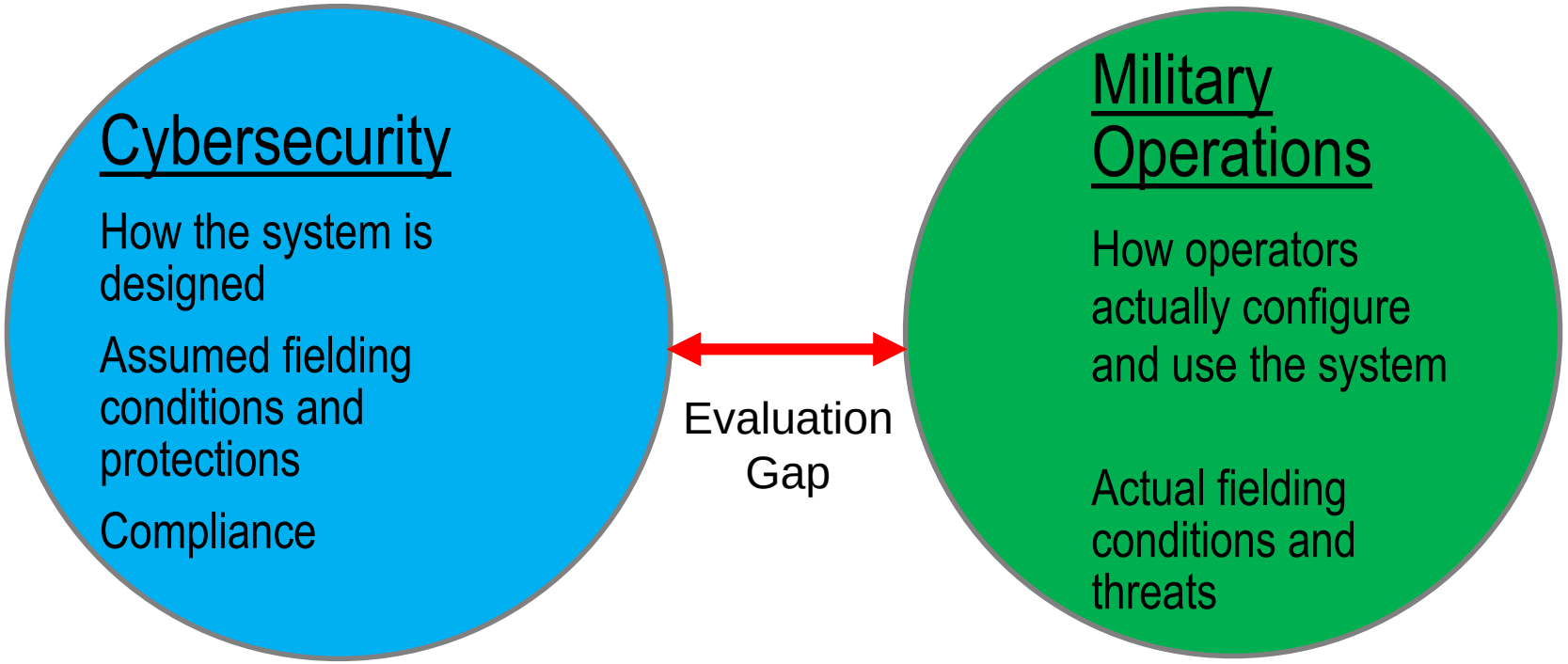
What We Really Want to Find Out from T&E

- Title X: Operational Effectiveness, Suitability, and ***Survivability***
- DOT&E Policy: Protect, Detect, React, Restore
  - Vulnerabilities and operational impacts
- System Survivability KPP Cyber Endorsement: Protect, Mitigate, and Restore
- Survivability COI: resilience and robustness against threats

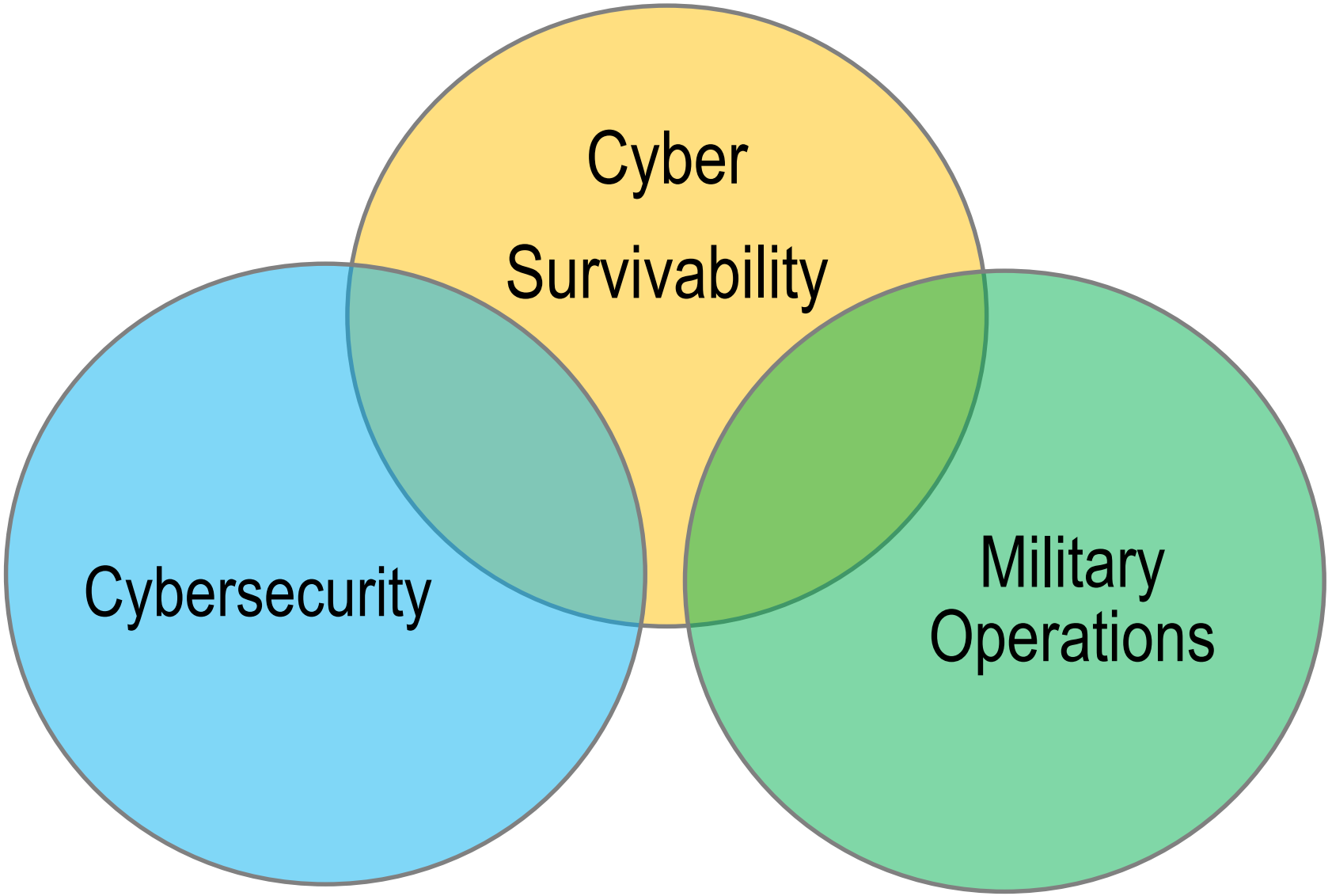
Definitions of Key Terms

- **Cyberspace:** "global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers." JP 3-13
- **Cybersecurity:** "Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation." DODI 8500.01
- **Survivability:** "the capability of military forces to avoid or withstand hostile actions while retaining the ability to fulfill their primary mission(s)." AR 73-1

Limitations of the term "Cybersecurity"



Cyber Survivability



System Survivability KPP Cyber Endorsement

- Cyber Survivability Endorsement IPT published implementation guide
- Attempts to help craft relevant and meaningful survivability requirements for the cyber domain
- Leverages RMF but not limited to RMF
- Creates categories based on mission and risk
- Three KPP pillars of “prevent, mitigate, and recover”

Proposed Critical Operational Issues and Criteria

- Critical Operational Issue: Does the system provide robustness and resiliency against hostile activity?
- Criteria
  - Meets all Federal and DOD Cyber security regulations, guidelines, and practices.
  - Introduces no new Medium/High to High risk exploitable cyber vulnerabilities to the networks and systems with which it interoperates.
  - While access to the system may fail under hostile action, it provides the ability to detect a loss of system integrity and provides the ability to restore the system and data to a known good state.

Conclusion

- The T&E community should stop using the term “cybersecurity” when what we mean is “cyber survivability.”
- Current and emerging policies and regulations concern themselves with cyber survivability and not just cybersecurity.
- “Cybersecurity” is a vague and potentially misleading term for senior leadership with limited expertise in that area.
- We’re already evaluating “cyber survivability”; we just haven’t been consistently using the right term.

Questions?

www.pinterest.com

Backup

Cybersecurity Is Important, But…

- It means different things to different people
  - RMF Compliance to get ATO
  - Protection against cyber threats
- Doesn't translate well beyond traditional IT systems
  - Modern militaries fight with networked weapon systems
  - Security controls are a best-guess effort and threats will find and exploit any false assumptions made in implementation
  - Operational impact of combat systems vastly different than impacts of traditional IT systems
- It can be mistaken as a discrete attribute that a system either has or doesn't have
  - Perception that efforts are futile
  - Falsely believing a system can be secure

Cyber Survivability

- In line with shift to defining cyberspace as a domain of warfare
- Emphasizes operational impacts
- Addresses JROC System Survivability KPP Cyber endorsement
- Remains in line with DOT&E policy

Cybersecurity vs. Cyber Survivability

Cybersecurity

- Adequacy of technical attributes and procedural controls
- Focused on risk identification and management

Cyber Survivability

- Ability to survive in the cyber domain
- Focused on impacts to mission(s) systems support/enable